variety of interfaces are possible. By way of example, the card reader interface **130** may provide a contact interface, a close-coupled interface, a remote-coupled interface, or a variety of other interfaces. With a contact interface, signals from the card are routed to a number of metal contacts on the outside of the card which come in physical contact with similar contacts of a card reader device. Depending on the application, the biometrics interface **110** can be separated from or combined with the card reader interface **130**.

[**0035**] In one embodiment, the smart card **100** includes components to perform the functions of biometric data analysis, random key generation, one-way hash function to generate a message digest, and encryption using a private key to generate a cipher text from a clear text.

[**0036**] The smart card **100** can be used to add a cipher hash digest to a message sent by the user. The hash digest is encrypted with a private key which is randomly generated by the card when the biometrics registration process performed by the card is complete.

[**0037**] The generation of random private and public keys can utilize well known algorithms and calculations to create the public and private keys. In the case of RSA, the encryption operation selects two prime numbers p and q and an exponent e which is relatively prime to $(p-1)(q-1)$. The private key is the composite number $n=p*q$ and the exponent e. To speed up the RSA algorithm, three common choices for e are 3, 17 and 65537.

[**0038**] The public key is the composite number n and the exponent d, so that $e*d$ is congruent to 1 modulo $(p-1)(q-1)$. The calculation of d is straightforward using the extended Euclidian algorithm.

[**0039**] A simple algorithm to generate the public and the private key on the card module runs as follows: first generate two large random prime numbers p and q and choose e among 3, 17 and 65537 so that e is relatively prime to $(p-1)(q-1)$; if not possible repeat the random prime numbers generation until two suitable primes are found; then calculate n and d. The generation of the two random prime numbers p and q can be achieved by using standard algorithms to generate probable primes with an acceptable very low probability of error, such as the Miller-Rabin algorithm, or provable primes, such as the Maurer's algorithm.

[**0040**] Various other algorithms are currently used for efficient asymmetric cryptography. In the Rabin algorithm one has to choose first two primes p and q congruent to 3 modulo 4. These primes are the private key, the product $n=p*q$ is the public key.

[**0041**] In the ElGamal algorithm to generate a key pair, one has to choose a prime p and two random numbers g and x such that both numbers g and x are less than p. The private key is x, the public key is g exp x modulo p, g and p.

[**0042**] It is clear that in all these cases the private and public keys can be generated by the cryptosystem processor **138** by generating random integers and prime numbers and performing relatively simple and rapid tests and calculations.

[**0043**] The advantage of this approach is that nobody, even the user, is able to know the private key **224**. The private key **224** is generated only when the biometric template data for the biometric registration is complete. The private key **224** is be embedded into tamperproof portion of the smart card **100** and is therefore inaccessible to any outside user.

[**0044**] The public key **220** is usually transmitted with a digital certificate. A digital certificate is a data package that completely identifies an individual and is issued by a certification authority only after that authority has verified the individual's identity. The data package includes the public key that belongs to the individual. When the sender of a message signs the message with his private key, the recipient of the message can use the sender's public key (retrieved from the certificate either sent with the message or available elsewhere on the network) to verify that the sender is legitimate. A certificate can also be used to send an encrypted message to the certificate owner by using the public key contained in the certificate.

[**0045**] The public key **220** generated by the smart card **100** can be used to generate a digital certificate by a certification authority. For example every smart card can be identified by a serial number. The certification authority can maintain records identifying which smart card **100** has been attributed to which individual and receive the public key corresponding to said smart card and said associated user upon the biometrics registration process.

[**0046**] As an example, The X.509 protocol defines the following structure for public-key certificates, and can be used directly with the smart card data:

Version
Serial Number
Signature Algorithm
Issuer Name
Period of Validity
1. Not Before Date
2. Not After Date
Subject Name
Subject's Public Key
Algorithm
Public Key
Extensions
Signature

[**0047**] The version field identifies the certificate format. The serial number is unique to the smart card **100**. The signature algorithm identifies the algorithm used to sign the certificate. The issuer field contains the name of the certification authority. The period of validity field includes a pair of dates that identifies the period of time that the certificate is valid. The subject field stores the name of the user to whom the certificate is issued. The subject's public key field includes the algorithm name and the public key itself. The last field contains the certification authority's signature.

[**0048**] In one embodiment of the invention, generation of the digital signature requires the combination of receipt of individual specific biometric data and the card specific private key. No one, even the user or the card manufacturer, is able to produce a second card generating the same private key. The smart card **100** is unique and specific to the user.

[**0049**] One of the advantages of the smart card **100** is that it safeguards against forgery in case of loss of the card or attempts to duplicate the smart card **100**. First, the smart card **100** is useless without its user. Second, the duplication of the